# Identity Management System PIA

## 1. Contact Information

**A/GIS Deputy Assistant Secretary**
Bureau of Administration
Global Information Services

## 2. System Information

(a) Name of system: Identity Management System

(b) Bureau: Diplomatic Security

(c) System acronym: IDMS

(d) iMatrix: #1000

(e) Reason for performing PIA: IDMS upgraded from Version 01.04.00 to Version 02.00.01.

- ☐ New system
- ☒ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

The purpose of this modification is to upgrade the core software set from AuthentX, version 4.0 to AuthentX, version 5.0; upgrade the dedicated client appliance hardware from ASA 1000s (embedded XP based) to ASA 2000s (embedded MS Windows 7 based); and to upgrade the server appliance hardware. In addition, XaNode (circa 2006) upgraded to XaNode (circa 2014) New Authentication Authority – server relay appliance.

## 3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒ Yes
☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

Authorization of an ATO extension was granted with an expiry date of 11/30/2020.

(c) Describe the purpose of the system:

The primary purposes of the system are to: (a) ensure the safety and security of Department of State facilities, systems, or information, and its occupants and users; (b) verify that all persons entering federal facilities, using federal information resources, or accessing classified information are authorized to do so; and, (c) track and control PIV cards issued to persons entering and exiting the facilities, using systems, or accessing classified information.

The Identity Management System (IDMS) is a database application that stores personally identifiable information (PII) collected from Department of State (DoS) direct-hire and contractor employees, requiring a Personal Identity Verification (PIV) smart card. The information collected facilitates the production (printing) and encoding (data elements required for physical/logical access and verification of the cardholder) of the DoS PIV smart card ultimately issued to an approved cardholder.

In addition, and to facilitate required facility access using Facility Access Cards (FACs), information is collected on: Foreign Service Nationals (FSNs); Locally Employed Staff (LESs); and, Eligible Family Members (EFMs).

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The IDMS processes and stores the following PII on all Department of State (DoS) direct-hire and contractor employees, Foreign Service Nationals (FSNs); Locally Employed Staff (LESs); and Eligible Family Members (EFMs).

- Names of Individuals;
- Date and Place of Birth of Individuals;
- Social Security Number (SSN) or Employee's Unique ID Number;
- Phone Number(s) of Individuals;
- Business Address(es) (when applicable);
- Personal Address;
- Government E-mail Address(es) of individuals who are issued a PIV or FLAC identification card; the FAC identification cardholders do not require a government appointed email address as they only require physical access to DoS facilities;
- Images or Biometric IDs (photographs and electronic fingerprints);
- Armed Forces Number (when applicable);
- Citizenship;
- Gender;
- Emergency Contact Information (name and phone numbers only);
- Organization/office of assignment (Collected on EFMs and FSNs upon employment at Post by DoS for FLAC/FAC issuance);
- Company name (Collected on EFMs and FSNs upon employment at Post by DoS for FLAC/FAC issuance);
- Copies of documents used to verify identification such as passport, driver's license number, national identification number, and birth certificates or information derived from those documents such as document title, document issuing authority, document number, document expiration date and other document information;

- Electronic Data Interchange Personal Identifier (EDIPI) known as the State Global Identifier (SGID);
- Personal Identity Verification (PIV) card issue and expiration dates;
- Personal identification number (PIN);
- PIV request form;
- PIV registrar approval signature;
- PIV card number;
- Emergency responder designation (if applicable);
- Level of national security clearance and date granted;
- Computer system user name;
- Authentication certificates; and
- Digital signature information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 CFR 731 - Office of Personnel Management (OPM) part 731, Suitability
- Executive Order 12333 (or any successor order);
- National Security Act of 1947, as amended;
- CIA Act of 1949, as amended;

For SSN collection:

- Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004;
- Federal Property and Administrative Act of 1949, as amended.
- Executive Order 10450 – Security Requirements for Government Employees;
- Executive Order 12829 – National Industrial Security Program; 5 United States Code (U.S.C.) 301; Federal Information Security Act (Pub. L. 104–106, sec. 5113);
- 5 Code of Federal Regulation (CFR) Office of Personnel Management (OPM) part 731, Suitability.
- Federal Information Processing Standards Publication (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒ Yes, provide:

- SORN Name and Number: Statement of Record Notice (SORN) - STATE-36, Security Records, which incorporates the Identity Management System (IDMS).
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

☐ No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-11-014-16a-16g
- Length of time the information is retained in the system: Temporary: Delete/destroy 20 years after separation, or transfer of cardholder from the Department of State.
- Type of information retained in the system:

Information retained in the IDMS, includes the following data fields:

- Names of Individuals;
- Date and Place of Birth of Individuals;
- Social Security Number (SSN) or Employee's Unique ID Number
- Phone Number(s) of Individuals;
- Business Address(es) (when applicable);
- Personal Address;
- Government E-mail Address(es) of individuals who are issued a PIV or FLAC identification card; the FAC identification cardholders do not require a government appointed email address as they only require physical access to DoS facilities;
- Images or Biometric IDs (photographs and electronic fingerprints);
- Armed Forces Number (when applicable);
- Citizenship;
- Gender;
- Emergency Contact Information (name and phone numbers only);
- Organization/office of assignment (Collected on EFMs and FSNs upon employment at Post by DoS for FLAC/FAC issuance);
- Company name (Collected on EFMs and FSNs upon employment at Post by DoS for FLAC/FAC issuance);
- Copies of documents used to verify identification such as passport, driver's license number, national identification number, and birth certificates or information derived from those documents such as document title, document issuing authority, document number, document expiration date and other document information;

- Electronic Data Interchange Personal Identifier (EDIPI) known as the State Global Identifier (SGID);
- Personal Identity Verification (PIV) card issue and expiration dates;
- Personal identification number (PIN);
- PIV request form;
- PIV registrar approval signature;
- PIV card number;
- Emergency responder designation (if applicable);
- Level of national security clearance and date granted;
- Computer system user name;
- Authentication certificates; and
- Digital signature information.

**4. Characterization of the Information**

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public (i.e., EFMs that are U.S. Citizens requiring facility access to government facilities)
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒ Yes ☐ No

- If yes, under what authorization?
- Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- 5 Code of Federal Regulation (CFR) Office of Personnel Management (OPM) part 731, Suitability;
- 5 United States Code (U.S.C.) 301; Federal Information Security Management Act (FISMA);
- Executive Order 10450 – Security Requirements for Government Employees; and
- Executive Order 12829 – National Industrial Security Program.

(c) How is the information collected?
The information is collected electronically for biometrics (i.e., fingerprints and photographs) and interactively from, or on, forms filled out by the individual requiring the DoS Personal Identification Card (e.g. PIV, FLAC or FAC). These forms include:
• DS-1838: Request for Personal Identification Card (PIV, FLAC or FAC).
• DS-7783: Overseas One Badge Application (FLAC or FAC)
• SF85: Questionnaire for Non-sensitive Positions;

• SF85P(S): Questionnaire for Public Trust Positions; and
• I-9: Employment Eligibility Verification.

(d) Where is the information housed?
☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.
N/A.

(e) What process is used to determine if the information is accurate?
The information is verified by the individual applicant.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Yes. The information is vetted and verified by the individual applicant at original enrollment and upon badge reissuance to ensure it remains current.

(g) Does the system use information from commercial sources? Is the information publicly available?
No. The information used by the IDMS is not sourced from publicly available or commercial sources.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes. A Privacy Act Statement is provided on the following forms, which provides notice to the individuals prior to the collection of his or her information. Additional notice is given through the publication of a System of Record Notice, State-36, Security Records. These forms include:
• DS-1838: Request for Personal Identification Card (PIV, FLAC or FAC); and
• DS-7783: Overseas One Badge Application (FLAC or FAC).
• SF85: Questionnaire for Non-Sensitive Positions;
• SF85P(S): Questionnaire for Public Trust Positions; and
• I-9: Employment Eligibility Verification.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒ Yes ☐ No
The individuals are informed on the DS-1838, Request for Personal Identification Card (PIV, FLAC or FAC) form and the DS-7783, Overseas One Badge Application (FLAC or FAC) form, in the Privacy Act Statement disclosure section that providing the information, including applicant's social security number is voluntary. However, failure to provide the

information requested on the form may result in an individual not being issued a Department of State Personal Identification Card.

- If yes, how do individuals grant consent?

In accordance with guidance in System of Records Notice (SORN) STATE-36, the individual may grant DS consent, by completing the form and signing it. These forms include:

- DS-1838: Request for Personal Identification Card ((PIV, FLAC or FAC);
- DS-7783: Overseas One Badge Application (FLAC or FAC);
- SF85: Questionnaire for Non-sensitive Positions;
- SF85P(S): Questionnaire for Public Trust Positions; and
- I-9: Employment Eligibility Verification.

- If no, why are individuals not allowed to provide consent?

N/A.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The privacy concerns are that more PII will be collected on an individual than is needed to verify authenticity. However, to alleviate this concern, the IDMS collects only the absolute minimum amount of PII required to satisfy the statutory purpose for collecting it and to satisfy DoS mission requirements. Collecting only the minimum amount of PII needed ensures that unnecessary risk to DoS personnel is minimized, and the exposure profile of the data collected and maintained is lowered by using only what is necessary to create a unique identifier.

## 5. Use of information

(a) What is/are the intended use(s) for the information?

The information collected in the IDMS is intended to be used for issuance of the DoS personal identification cards used to control physical and logical access to DoS owned or leased facilities and information systems. The information collected is not used for any other purpose.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. The information solicited on the forms, including the applicant's social security number, is used to conduct appropriate National Agency Check with Written Inquiries (NACI) or higher federal background investigations prior to issuing a Department of State personal identification card in accordance with the Federal Information Processing Standards Publication (FIPS) 201-2 *Personal Identity Verification (PIV) of Federal Employees and*

*Contractors.*

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
(2) Does the analysis result in new information? ☐Yes ☐No
(3) Will the new information be placed in the individual's record? ☐Yes ☐No
(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

## 6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The IDMS server enclave has an established internal connection to the OpenNet/Active Directory (AD) service via hypertext transfer protocol secure (HTTPS) protocol to retrieve the User Principal Name (UPN) for encoding on the DoS personal identification badge by the IDMS. In return, the IDMS is providing AD the EDIPI and the PIV certificate being encoded on the DoS credential (badge).

(b) What information will be shared?

- UPN; and
- EDIPI.

(c) What is the purpose for sharing the information?

Suitability and identity vetting of Dos direct-hire and contractor employees as well as Foreign Service Nationals (FSNs); Locally Employed Staff (LESs); and Eligible Family Members (EFMs) who require facility access using Facility Access Cards (FACs).

(d) The information to be shared is transmitted or disclosed by what methods?

The information to be shared is transmitted or disclosed by the following methods:
OpenNet/Active Directory (AD), iMatrix #634:
The IDMS enclave has an established internal connection to the OpenNet/AD service via hypertext transfer protocol secure (HTTPS) to retrieve the User Principal Name (UPN) for encoding on the DoS badge by the IDMS. In return, the IDMS is providing AD the Electronic Data Interchange Personal Identifier (EDIPI) and PIV certificate being encoded on the DoS credential (badge).

(e) What safeguards are in place for each internal or external sharing arrangement?

The information shared is safeguarded via the AuthentX server appliance, which includes security features such as: FIPS 140-2 approved encryption; Internet Protocols (IP) Routing

Tables (Firewall); and, the vendor-proprietary XTec™ Identity System (XIDS), which monitors system configuration hash values to detect and prevent unauthorized changes.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Unauthorized access to the IDMS, data leakage and information exposure are concerns identified by the Department of State. These risks are mitigated through adherence to and implementation of security controls in the IDMS system design and operation. Procedural and technical security controls, including permission and access controls, are in place to protect data in transit and at rest. Use of data encryption, audit log review, and separation of duties are some of the controls in place to mitigate the risk of data exposure.

The IDMS application is configured in a trusted enclave of server appliances operating separate from the OpenNet environment hosted in the Department of State data centers with controlled access in place.

Internal access to PII within IDMS is only available to authorized users who have been assigned to one of the following IDMS accounts to support the Department's mission and business functions: 1) end user accounts; 2) application administrator accounts; and, 3) system administrator accounts.

The Department has implemented the 5 FAM 469 "Rules of Behavior for Protecting PII" Policy which is to be adhered to by all workforce personnel to protect the PII they have access to in the performance of their official duties. The Information Security Modernization Act (FISMA) of 2014 requires system owners to ensure that individuals requiring access to information technology (IT) systems , including those containing PII, sign appropriate access agreements prior to being granted access. The access agreement for a system must include rules of behavior tailored to the requirements of the system.

The sharing of the data between the IDMS application and Active Directory as noted in section 6 (a) "Sharing of Information" follows the requirements of 5 FAM 469 through a Memorandum of Understanding between these systems in the sharing of PII.

## 7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

A DoS One Badge identification cardholder (e.g. PIV, FLAC, or FAC) cannot access their PII stored within IDMS directly, however the Department has the following procedures in place by which individuals may request access to records about themselves, request amendment or correction of those records, and request an accounting of disclosures of those records by the Department:

- The Department provides all applicants with a rights and responsibilities brochure at DOS One Badge, domestic and overseas, and One Badge issuing locations. This brochure provides applicants with background information on the purpose of

collecting their PII, the legal authorities for doing so, and their rights with regard to denial of a credential and their privacy.

- An applicant's information can be updated in the IDMS by an Enrollment Official via the re-enrollment process and the reissuance process. Two forms of identity source documents are required at time of enrollment for identity proofing IAW FIPS 201-2.
- Change procedures for notification and redress are also published in the System of Records Notice (SORN) – Security Records, STATE-36 and in rules published at 22 CFR 171.32: Subparts A and D provide the public with the requirements necessary to make a request for personal records and other information maintained by the DoS and Subpart D describes the procedures by which individuals may request access to records about themselves, request amendment of correction of those records, and request an accounting of disclosures of those records by the Department.

In order to process a request for personal information, the DoS requires the following checklist items:

- Full name (and any aliases) of the individual(s) who is/are the subject of the request
- Current Mailing Address
- Date of birth
- Place of birth (city and state/country)
- An adequate description of the records you are seeking
- Timeframe
- Origin of the records
- Citizenship Status
- Notarized signature or Under Penalty of Perjury Statement

Electronic submission requests are available at https://foia.state.gov/Request/Submit.aspx.

Under the rules published at 22 CFR 171.32, an individual can make a request for his/her own records by providing the following information to the Office of Information Programs and Services; A/GIS/IPS/RL; U.S. Department of State, SA-2; Washington, D.C. 20522-8100:

- Full name including distinguishing information (such as Dr., Jr., Sr., III); and any aliases or other names used (such as maiden name);
- Present mailing address;
- Date and place of birth;
- Types of records sought;
- Timeframe of record;
- Your original signature; and

- Any other information that might help in identifying the record such as social security number or passport number.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.

A One Badge cardholder can correct inaccurate or erroneous PII information contained within IDMS via the One Badge card reissuance workflow process for a PIV, FLAC or FAC identification card.

The One Badge cardholder must undergo the sponsor approval process submission (e.g., DS-1838, DS-7783) identity proofing and photographic portrait update. During the reissuance, a new record would not need to be created in the IDMS, and fingerprint capturing would only be required if biometric authentication fails or if the fingerprints stored in IDMS are more than 12 years old.

The One Badge cardholder is also able to update changes to their legal name, security clearance, employment status, and access requirements (logical and/or physical) as well using the established One Badge card reissuance process above.

For any other type of change, the notification and redress procedures are published in SORN-36, Security Records, which incorporates the IDMS, and in the procedure rules published at 22 CFR 171.33.

The procedures in 22 C.F.R. 171.32 inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act (5 U.S.C. 552a) provisions for notification and readiness may exist for certain portions of records on grounds pertaining to law enforcement and/or in the interest of national defense and foreign policy if the record have been properly classified. These exemptions are published as agency rules at 22 C.F.R. Part 171.32 Part C. Individuals should provide the appropriate evidentiary documentation to address errors in information.

If no, explain why not.

N/A.

(c) By what means are individuals notified of the procedures to correct their information?

- The Department provides all applicants with a rights and responsibilities brochure at DOS One Badge, domestic and overseas, One Badge issuing locations. This brochure provides applicants with background information on the purpose of collecting their PII, the legal authorities for doing so, and their rights with regard to denial of a credential and their privacy.
- Change procedures for notification and redress are also published in the System of Records Notice (SORN) – Security Records, STATE-36 and in rules published at 22 CFR 171.33 Subparts A and B provide the public with the requirements necessary to make a request for personal records and other information maintained by the DoS and Subpart D describes the procedures by which individuals may request access to records about themselves, request amendment of correction of those records, and request an accounting of disclosures of those records by the Department.

## 8. Security Controls

(a) How is the information in the system secured?

The information stored in the IDMS is secured via FIPS 140-2 encrypted products and is protected in a firewalled, trusted enclave that is separate from the OpenNet operating environment.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Only authorized, cleared DoS direct-hire and contractor employees are given user access to the IDMS application. DoS direct-hire and contractor personnel are subject to a rigorous background investigation by the diplomatic security service and are vetted for need-to-know and facts that may bear on the individual's loyalty and trustworthiness.

Users of the IDMS application fall into three categories: 1) End Users; 2) Application Administrators; and, 3) System Administrators. User access to the IDMS application is role-based, which enforces separation of duties and least privileged access. User access, authorizations and permissions are granted at a level commensurate with assigned roles and need-to-know for each user and only at the level necessary for each user's function.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Audit logs are maintained separately and are used to record system and user activity, including invalid logon attempts and access to data. The IDMS Senior Systems Administrator monitors audit logs daily for unusual activity.

(d) Explain the privacy training provided to authorized users of the system.

The Department of State's requires all new employees and contractors to complete a Cybersecurity Awareness Course (PS-800), which has a privacy component. Authorized users of IDMS are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training annually in order to retain access. Prior to accessing the system, the Enrollment and Issuance officials of the IDMS system are trained on protecting personally identifiable information whether they be direct-hire or third-party contractor employees. Users, whether they be direct-hire or contractors, must receive a Departmental information system security briefing and pass a quiz prior to receiving access to a DoS network. Foreign Service, Civil Service and Locally Employed Staff that handle PII must take PA-459, *Protecting Personally Identifiable Information*. DS/SI/CS has a Departmental Security Awareness program in-place.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

Access, authorizations, and permissions to the PII in IDMS are granted at a level commensurate with the user's need to know and only at the level necessary for management of the data.

The PII collected and maintained has resulted in a security categorization of "HIGH" for the PII contained within IDMS, which requires specific privacy and security controls. The controls are subject to rigorous testing, a formal assessment and authorization process, and an acceptance of related privacy risks prior to receiving an authority to operate. In an attempt to mitigate these risks, the Department of State has implemented management, operational, and technical security controls to protect the PII in IDMS in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology.

These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software) and audit reports.

(f) How were the security measures above influenced by the type of information collected?

Based on the type of information collected by the IDMS application, the overall security categorization of the system is high at the data impact level for information types as determined by the Federal Information Processing Standard Publication 199, *Standards for*

*Security Categorization of Federal Information and Systems*, and implemented security controls commensurate with that categorization.

## 9. Data Access

(a) Who has access to data in the system?

Only authorized, cleared DoS direct-hire and contractor employees having a need-to-know are allowed access to the IDMS application. Users of the IDMS application fall into three categories: 1) End Users; 2) Application Administrators; and, 3) System Administrators. User access to the IDMS application is role-based, which enforces separation of duties and least privileged access.

(b) How is access to data in the system determined?

Access to the data in the IDMS is determined by assigned roles (separation of duties) by the IDMS Director of Operations, and access is allowed only on a need-to-know basis.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒ Yes ☐ No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No. Access to the IDMS is restricted to authorized personnel having a need-to-know and is further restricted by being role-based.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

NIST SP 800-53, Revision 4, Auditing (AU) family of controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by users having authorized access to the data.

AU-2 and AU-12 security control audit logs are maintained on the IDMS servers to effectively trace actions affecting the security of the system to the responsible individual.

For each recorded event, the IDMS audit record captures the computer operators and system administrator's full name, date and time a user's record was accessed, as well as changes made to the record, and the role of the user who accessed the record. Audit logs are used to secure the system and prevent unauthorized users from accessing the system.

The log is protected from unauthorized modification, destruction, and access by the limited rights assigned by the system administrator using the IDMS operating system software.